Software Development Life Cycle (SDLC) Policy (4300-0003)

Final September 4, 2013

1.1 Purpose

The purpose of this policy is to establish a standard expectation for implementation of a Software Development Lifecycle (SDLC) that produces software that is secure, accessible, mobile ready, and compliant with State development standards, policies, and practices.

1.1.1 Scope

The scope of this policy includes all DTS employees, contractors, and temporary workers involved in the development of State software.

1.1.2 Background

The SDLC must address common business and development phases to be effective across the enterprise, and must address key issues of security, accessibility, mobile device access, and standards compliance.

1.1.3 Exceptions

A business case for non-compliance must be established and the request for exemption approved in advance through a risk acceptance process where the Chief Information Officer or authorized designee is notified and approval for the exception is granted.

1.2 Policy

Software development projects must address the following areas in a manner consistent with standard agency and DTS business and development practices. All seven SDLC phases must be addressed and incorporated in a consistent manner. Agencies and developers may make necessary adaptations based on the size and complexity of projects. Policy implementation may incorporate agency standards and guidelines that may be more stringent than the control points or phases identified in this SDLC.

1.2.1 Phase 1. Preliminary Analysis: Based upon a stakeholders initiation request, the objective of this phase is to conduct a preliminary analysis, propose alternative solutions, describe costs and benefits and submit a preliminary plan with recommendations.

- ***Conduct the preliminary analysis:*** In this step, document the agency's objectives and the nature and scope of the problem under study.
- ***Propose alternative solutions:*** In digging into the agency's objectives and specific problems, some solutions may already be evident. Alternate proposals may come from interviewing employees, clients, suppliers, and/ or consultants. With this data, there are five choices: leave the system as is, improve it, develop a new system, or adapt a system from another agency or State, or purchase a commercial application.
- ***Describe the costs and benefits.*** Look at tangible costs versus tangible and intangible benefits. Address the benefits of new development versus improvements to existing systems, adaptations of other agency or State systems, or doing nothing, or purchasing a commercial solution.

- ***Identify risks:*** Every project or task has risks. Cost, time, implementation, security, privacy and regulatory risks may be identified. Risk reduction and mitigation plans are to be considered as part the preliminary analysis of any development effort
- ***Agency and DTS budget approval***. Obtain management and financial approval for the project, and add pertinent business case documentation as required.

1.2.2 Phase 2. Systems analysis, requirements definition: Defines project goals into defined functions and operation of the intended application. Analyzes end-user information needs. Address requirements for security, mobility, accessibility, and platform use expectations.

1.2.3 Phase 3. Systems design: Describes desired features and operations in detail, including screen layouts, business rules, process diagrams, pseudo code and other documentation. Depending upon the size of the project, prototyping is useful in this stage. Larger complex projects require more definition and more controls. Smaller projects may move directly to faster methodologies.

1.2.4 Phase 4. Development: Actual development of code, preferably in functional components that can be tested separately. Apply State standards such as:

- ***Accessibility:*** Applications need to be delivered and compliant with State accessibility guidelines at http://utah.gov/accessibility.html and Utah Web Standards and Guidelines: Part 4.0, Accessibility
- ***Privacy:*** Application implementation and data collection need to be compliant with State Privacy Policies at http://www.utah.gov/ privacypolicy.html
- ***Security:*** Applications must be deployed within a secure hosting environment, and be compliant with the State Security Policy.
- ***Mobility and Usability:*** Applications need to be deployable in any major browser. Applications need to be responsive and usable on desktop and mobile devices and consistent with the Utah Mobile Strategy and Mobile Platform Design Guidelines.
- ***Web Standards:*** Web implementation of applications need to be compliant with 4300-0001-1 Web Standards and Guidelines; and associated design documentation.

1.2.5 Phase 5. Integration and testing: Brings all the pieces together into a testing environment, then checks for errors, bugs and interoperability, accessibility, mobility, performance, standards compliance, and an independent security review.

- ***AccessibilityTesting***
- ***Environment, Integration, and System Testing***
- ***User Interface and Unit Testing***
- ***Load Testing and Performance Tuning***
- ***Privacy Policy Compliance***
- ***Security Code Testing***
- ***Mobility and Usability Testing***
- ***Standards Compliance Testing***

1.2.6 Phase 6. Acceptance, installation, deployment: The final stage of initial development, where the software is put into production and runs actual business. This is the final checkpoint on architectural compliance, application and hosting security. Development (DEV), Acceptance (AT), and Production (PROD) environments must be physically separate instances on different servers.

1.2.7 Phase 7. Maintenance Plan: What happens during the rest of the software's life: changes (compliance with State Change Control policies), corrections, additions, moves to a different hosting platform, decommissioning, and more.

1.3 Enforcement

Software development managers and their contractors and staff are accountable for SDLC implementation. Violation of this policy may be the basis for discipline including but not limited to termination. Individuals found to have deliberately violated this policy may also be subject to legal penalties as may be prescribed by State and/or federal statute, and/or regulation. Funding of future software development projects may be withheld if the requirements of these processes are not followed.